IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF A BLACK TCL MODEL A509DL MOBILE PHONE IMEI 015858001917651, TELEPHONE NUMBER (801) 708-1855, USED BY TRAVIS RYAN MARTIN, CURRENTLY LOCATED AT THE SALT LAKE CITY FBI FIELD OFFICE	Case No. 2:22mj65-DAO

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent (SA) Matt Larson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic Device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent of the Federal Bureau of Investigation (FBI) for over twenty years. Prior to FBI service, I was a Police Officer for six years. During 26 years of continuous law enforcement experience I have investigated violations of various federal and state laws including matters related to homicide, rape, child sexual assault, aggravated robbery, aggravated assault, bank robbery, organized crime, drug trafficking, money laundering, firearms trafficking, and the exploitation of children in several jurisdictions which have resulted in hundreds of felony prosecutions and convictions. In the course of these investigations I have utilized or participated in a variety of traditional and sophisticated investigative techniques to

include undercover operations; online undercover operations; wire taps; pen registers; consensual recordings; interviews and interrogations; recruitment and deployment of informants; search warrants for a variety of evidence to include searches of smart devices, mobile telephones, computers and internet applications; and analysis of evidence contained in telephone records, smart devices, and internet applications. I am currently assigned to an FBI Child Exploitation Task Force where my duties include conducting covert online investigations to identify preferential sex offenders targeting juveniles. I have also received training and gained experience over the years with internet related investigations as criminal suspects have increased the use of internet tools to facilitate criminal conduct. In addition, I have owned and used smart devices, mobile telephones, and computers on a daily basis for years and have gained familiarity with them through daily use**.**

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a black TCL MODEL A509DL Tracfone mobile telephone, IMEI 015858001917651, currently assigned telephone number (801) 708-1855, hereinafter the "Device," found in the possession of TRAVIS RYAN MARTIN at the time of his arrest on November 19, 2021. The Device is currently located at the Salt Lake City FBI Field Office.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On September 22, 2021, TRAVIS RYAN MARTIN (MARTIN) used the Facebook messenger feature of his Facebook account to contact the Facebook account of a notional 15 year old boy (hereinafter referred to as "the boy") in Tennessee operated by an FBI Online Undercover Employee (UCE) in Knoxville. From September 22 through 27, 2021, MARTIN sent the boy close up pictures of his erect penis, his scrotum and his anus taken in a manner consistent with someone using a mobile telephone to take pictures of himself. He asked the boy to produce pictures of his own penis and anus and distribute them to MARTIN; asked the boy to be his boyfriend; asked the boy to swallow MARTIN'S "cum semen," made several other graphic comments about sex acts he wanted to do to the boy such as he wanted to spread the boys butt cheeks and "finger fuck" him, and stated he was at a trucking school in Utah getting a CDL (commercial driver license) after which he would travel to Tennessee for the purpose of having sex with the boy. MARTIN also provided the boy the telephone number (801) 708-1855 and asked to speak with the boy by telephone. MARTIN indicated in his messages that he had tried to call the boy but the boy did not answer.

7. I reviewed MARTIN'S criminal history and noted a prior felony conviction in 2003 for sexual assault of a child under 16 in Idaho. I also reviewed his sex offender registration in Utah that indicated he was a student at the Utah Trucking Academy in Salt Lake City. In response to a subpoena, Facebook returned information on October 10, 2021, provided by MARTIN when he registered for his account. MARTIN provided the telephone number (801) 708-1855 during registration. I reviewed the portions of his Facebook account MARTIN had made available for any member of the public to view. I noted almost every one of his Facebook

"friends" were young males who shared the same general physical traits: juvenile or similar in appearance to a juvenile boy, slender, dark hair, with no body hair.

8. On November 17, 2021, a grand jury seated in the District of Utah, United States District Court, returned a true bill of indictment and the court issued an arrest warrant that charged MARTIN with violations of the following statutes: 18 USC § 2251 (a) and (e), Production of Child Pornography; 18 USC § 2422 (b), Coercion and Enticement for Illegal Sexual Activity; 18 USC § 1470, Transfer Obscene Matter to a Minor.

9. On November 19, 2021, I arrested MARTIN as he arrived at the Utah Trucking Academy in Salt Lake City. I searched him incident to arrest and located the Device in his right front pants pocket. I transported the Device to the Salt Lake City FBI Field Office where it has remained.

10. During a post-Miranda interview MARTIN confirmed the following information. The telephone number of the Device I found in his pocket is (801) 708-1855. He has been in the state of Utah and has not left the state for over two years. He started attending the Utah Trucking Academy on September 20, 2021 and was in the Salt Lake City area throughout the time between September 20, 2021 and his arrest. After I showed him a recording of communications between him and the UCE which included screen captures of the Facebook account the UCE communicated with, MARTIN confirmed that account was his Facebook account. He used the Device to take the pictures that appear in his communications with the boy.

11. He does not remember communicating with that boy, but he has sent the same pictures to other individuals he has communicated with on the Device in the Facebook

messenger application. He admitted he has communicated with young teenage boys on Facebook and that it seemed like a bad idea given he has been convicted of sexually assaulting a 15 year old boy. He said he has deleted some of his communications. For example, he said he communicated with an 11 or 12 year old boy but he deleted that chat. MARTIN claimed he had no way of knowing how old people he chatted with actually were unless they showed him identification. He agreed that if he had a teenage child he would not want a grown man to communicate with his child the way he had with Facebook friends who told him they were juveniles. MARTIN said he was released from prison three years ago after serving all of a 15 year sentence.

12. MARTIN gave his consent for me to look through his Facebook account on the Device. He signed a consent form after being advised he was not required to consent to the search. He unlocked the Device so I could look through it. He later provided the unlock code to me as well. I noted that MARTIN does in fact have the Facebook application downloaded on the Device. I noted as I looked at his Facebook communications that MARTIN had exchanged messages about sex with other Facebook users, many of whom were similar in appearance to juvenile boys, some of whom told MARTIN they were under 18 and that MARTIN sent some of them pictures of his genitalia similar to those he sent the UCE. MARTIN had used his Facebook application to access Facebook and chat with other Facebook accounts as recently as two days before his arrest. I also noted that in some of the chats, MARTIN discussed sending money to the other FaceBook user. Considered in context, financial payments made by MARTIN to FaceBook users who may be juvenile boys requires additional investigation as possible payments in exchange for child pornography if not for actual access to children so that MARTIN can sexually assault them. Based on my training and experience considered in light of the facts in this

affidavit I believe probable cause exists to search financial records and documentation of financial transactions found on the Device.

13. I know based on my training and experience that electronic devices like the mobile telephone seized from MARTIN can be used to take and store photographs. They can also be used to store copies of photographs and videos sent to the user of the device so that the user can access and view the photographs or videos at any time. They can be used to take "screen shots" or "screen captures" which are simply pictures of whatever is displayed on the screen of the device when the photograph or video recording of it is made. These files can be stored on the device indefinitely like any other photograph, picture or video.

14. MARTIN has previously been convicted of sexually assaulting a 15 year old boy. He was recently charged by grand jury indictment in this district for conduct related to contacting someone he evidently believed to be a 15 year old boy, soliciting the production of child pornography by that boy, and arranging to mee that boy and have sex with him after he finished instruction at the Utah Trucking Academy. This pattern combined with what I have already seen on the Device seized from him and statements he made during his post-arrest interview viewed in light of my training and experience regarding sex crimes leads me to believe he was at the time of his arrest involved in a recurring pattern of criminal behavior centered on the sexual exploitation of children which was only stopped due to his arrest.

15. I know from training and experience that sexual predators like MARTIN who prey on children often use electronic devices to access, download, share, produce, and retain child sexual assault material (CSAM) or child pornography for continued viewing. Electronic devices like the one seized from MARTIN allow sex offenders to store evidence of their crimes

against children and evidence of crimes against children committed, recorded and shared by other sex offenders. Such devices can also be used to access, share, and copy such material from remote servers, directly from the devices of other pedophiles or from other devices accessible to the user such as their desk top computers, lap top computers or other electronic devices. Given that MARTIN urged the notional boy in this case to produce and distribute CSAM and is a convicted child sexual predator and that he has contacted other Facebook users who are similar in appearance to juvenile boys I believe it is reasonable to assume he may have used his Device to make similar demands from other children and therefore evidence of crimes against children may at this time be stored on his device, even if he believes he has deleted it.

16. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession when TRAVIS RYAN MARTIN was arrested as described above and searched incident to arrest. The Device was in his right front pocket. Therefore, while the FBI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

17. The Device is currently in storage at the Salt Lake City Field Office of the FBI, 5425 West Amelia Earhart Drive, Salt Lake City, Utah, 84116. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless Device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the Device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage Device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the Device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication Devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a

personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic Device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic Devices that communicate with each other. Due to the structure of the Internet, connections between Devices on the Internet often cross state and international borders, even when the Devices communicating with each other are in the same state.

19. Based on my training, experience, and research, and from consulting the seller's advertisements and product technical specifications available online at https://www.tracfone.com I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, pager, portable media player, GPS navigation device, tablet and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device, where and when they used it to employ the Device's capabilities, the date and time various applications on the Device were opened or used, the content of text messages and attachments such as media files or pictures, and a variety of other information which establishes whether or not and how the Device was used to facilitate criminal activity.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives or internal memory storage—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. In at least some of his text communications with his FaceBook friends or other FaceBook users, MARTIN discussed sending money to them. Financial records stored on the phone may establish who was in possession of and using the Device when the listed offenses were committed, may help identify victims, may reveal payments made by MARTIN in exchange for child pornography, and may reveal his purchase of or use of applications to facilitate the listed crimes which have since been deleted. Through my training and experience I have learned internet applications ("apps") can be downloaded, used, and deleted after use to conceal or destroy evidence of criminal conduct that includes text messages and picture and video files. Many "free" apps require the user to provide financial information such as credit card, debit card or bank account information. Many apps solicit subsequent "in app" purchases which are made with the financial card or account information provided when the user registered the account. Other apps require an actual up front purchase expense. Financial records can provide documentation of which apps the user downloaded or purchased, when the device user used the Device to download apps, or buy more data or telephone call minutes, even after the apps and related accounts have been deleted by the user.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a Device can also indicate who has used or controlled the Device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an adult individual like MARTIN uses an electronic device to hunt for child victims to sexually exploit and assault the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense. In cases like the one described herein, the device may also contain and is likely to contain information which may assist in identifying and protecting child victims of sexual exploitation.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Matt Larson
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 on February 3, 2022:

Daphne A. Oberg
DAPHNE A. OBERG
United States Magistrate Judge

ATTACHMENT A

The property to be searched (hereinafter referred to as the Device) is a black TCL MODEL A509DL Tracfone mobile telephone, IMEI 015858001917651, telephone number (801) 708-1855, found in the possession of TRAVIS RYAN MARTIN at the time of his arrest. The Device is currently located at the Salt Lake City FBI Field Office.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC § 2251 (a) and (e), Production of Child Pornography; 18 USC § 2422 (b), Coercion and Enticement for Illegal Sexual Activity; and, 18 USC § 1470, Transfer Obscene Matter to a Minor and involve TRAVIS RYAN MARTIN including:

a. Contents and data stored in or in connection with any application on the Device capable of being used to communicate with juveniles in any way to include voice, text, or video communications or transmitting any media files such audio recordings, internet address links, pictures or videos.

b. Contact lists.

c. Media files such as pictures, photographs, videos or screen shots.

d. any information tending to identify or assist in the identification, location, or description of any child predator sexually exploitation children or any child victim of such crimes including but not limited to any biographical information, screen names, monikers, handles, user names, passwords, account names, email addresses or account information;

e. any information recording MARTIN'S location or travel as he used the device and indicating the location of any potential child victims whom MARTIN contacted or attempted to contact.

f. all bank records, checks, credit card bills, account information, and other financial records which indicate how he may have used the Device to facilitate violation of

the listed crimes, to include enticing minors to create or send child pornography, or which indicate his location when he violated the listed crimes, to include attempts, or which document application/app purchases or in-app purchases which relate to apps which could be used to facilitate the sexual exploitation of children. My training and experience has taught me that apps can be deleted from electronic devices so that other means such as financial records may be the only evidence that the suspect once possessed or used the app.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the Device connecting to the internet or to Internet Protocol addresses including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.